## Обратный остаток

Обратное по модулю целого a — это такое целое число x, что произведение ax сравнимо с 1 по модулю m.

**Теорема.** Если (a, m) = 1, то у a есть обратный остаток по модулю m.

- 1 Дано простое число p и его некоторый ненулевой остаток a.
  - (a) Докажите, что в последовательности  $0 \cdot a, 1 \cdot a, 2 \cdot a, \dots, (p-1) \cdot a$  все числа дают разные остатки по модулю p.
  - (b) Докажите, что существует и при том единственный обратный остаток b
  - (с) Какие остатки совпадают со своими обратными остатками?
- $\lfloor 2 \rfloor$  Какой остаток даёт x при делении 13, если:
  - (a)  $3x \equiv 4 + x \pmod{13}$ ;
  - (b)  $7x \equiv 8 + 3x \pmod{13}$ ;
  - (c)  $10x + 2 \equiv -x \pmod{13}$ ;
  - (d)  $6 \equiv 11 + 3x \pmod{13}$ ;
  - (e)  $-2x \equiv 1 + 3x \pmod{13}$ ;
- [3] (Теорема Вильсона.) Докажите, что  $(p-1)! \equiv -1 \pmod{p}$ , если и только если p является простым числом.
- $\boxed{4}$  Пусть p простое число и  $k \leqslant p$ . Докажите, что  $(p-k)!(k-1)! \equiv (-1)^k$ .
- [5] Пусть  $p \geqslant 3$  простое число. Докажите, что если сумму  $\frac{1}{1} + \frac{1}{2} + \ldots + \frac{1}{p-1}$  привести к общему знаменателю, то числитель получившейся дроби будет делиться на p.
- 6 Пусть числа p и p+2 являются простыми числами-близнецами. Докажите, что справедливо  $4((p-1)!+1)+p\equiv 0\pmod{p^2+2p}$ .
- [7] На доске написаны числа  $\frac{100}{1}, \frac{99}{2}, \dots, \frac{1}{100}$ . Можно ли выбрать какие-то девять из них, произведение которых равняется единице?
- [8] Докажите, что  $5^{70} + 6^{70}$  делится на 61.